

REMARKS

In response to the Office Action dated March 23, 2004, claims 1-4 and 6-28 remain in the application. Claim 5 has been canceled. Claims 1, 6, 9, 14, 17, 20, 21, and 24 are amended. No new matter has been introduced. Reexamination and reconsideration of the present application are respectfully requested.

In the Office Action dated March 23, 2004, the Examiner rejected claims 1-28 under 35 U.S.C. § 102 (e) as being anticipated by Jablon, U.S. Patent Application Pub. No. US2002/0067832 A1 (hereinafter Jablon). Applicants respectfully traverse the rejections.

Independent claim 1, as amended, now recites:

A method of accessing a password comprising:
dividing the password received from a client into a plurality of pieces;
storing each piece of the plurality of pieces of the password on a different one of a plurality of servers, each of the plurality of servers being independent from others of the plurality of servers;
separately authenticating a user at each of the plurality of servers, each of the plurality of servers transmitting the piece of the password stored at the respective server to the user when the authentication at that server is successful;
assembling the password from the password pieces transmitted from the plurality of servers; and
deleting the password and the plurality of pieces of the password from the client.

The Jablon reference discloses a system for providing improved password authentication using split keys among multiple machines. (*Jablon; Abstract*) Jablon describes a system wherein a private key U is split into three shares including a password derived share and two larger shares, X and Y. The shares of the private key U and a verifier function are used to provide secure communication between two users at separate machines. (*Jablon; paragraphs 20-21*)

The Jablon reference does not disclose, teach or suggest the method specified in

independent claim 1, as amended. Unlike the method specified in independent claim 1, as amended, Jablon does not teach a method that includes “*storing each piece of the plurality of pieces of the password on a different one of a plurality of servers, each of the plurality of servers being independent from others of the plurality of servers*. Instead, Jablon teaches a system in which Alice’s private key is split into three shares P, X and Y. (*Jablon; paragraph 21*) A verifier {g,V} is applied to Alice’s secret private key S, which results from the bitwise exclusive-or of two shares of Alice’s private key U and the exponentiation of Alice’s password derived share P. (*Jablon; paragraph 21*) The verifier and Y are then stored on the machine of the other party to the communication, Bob. Alice must memorize share P and must store X on her own machine. (*Jablon; paragraph 21*) As such, Jablon teaches that only some of the pieces of the private key U are stored on different machines, which is not the same as storing each piece of the plurality of pieces of the password on a different one of a plurality of servers.

In addition, the Jablon reference does not teach a method that includes “*deleting the password and the plurality of pieces of the password from the client*.” On the contrary, the Jablon reference discloses a system in which at least one share (P) of the split key is in fact stored on the client system. (*Jablon; paragraph 21*) Accordingly, Applicants respectfully submits that independent claim 1, as amended distinguishes over the Jablon reference.

Claims 2-4 are directly or indirectly dependent from independent claim 1, as amended. Accordingly, Applicants respectfully submit that dependent claim 2-4 distinguish over Jablon for the same reasons discussed above with respect to independent claim 1, as amended.

Independent claim 6, as amended, now recites:

A method of securely storing a password comprising:
receiving an encrypted portion of the password, the encrypted portion of the password comprising less than the entire password;
storing the encrypted portion of the password with identification information for a user

of the encrypted portion of the password;

receiving a request for the encrypted portion of the password, the request including the identification information; and

returning the encrypted portion of the password to the user when the identification information in the request matches the stored identification information.

The Jablon reference does not disclose, teach or suggest the method specified in independent claim 6, as amended. Unlike the method specified in independent claim 6, as amended, Jablon does not teach a method that includes ***“receiving an encrypted portion of the password, the encrypted portion of the password comprising less than the entire password.”***

Instead, Jablon teaches that a user creates n shares of a master symmetric key K_m . A symmetric key derived from the master symmetric key K_m is then used to encrypt the users private key U , *in its entirety*, resulting in an encrypted private key U_K . (Jablon; paragraph 82) This is not the same as receiving an encrypted *portion of the password*, the encrypted portion of the password comprising less than the entire password.

In addition, Jablon does not teach a method that includes ***“storing the encrypted portion of the password with identification information for a user of the encrypted portion of the password.”*** Rather, Jablon teaches that the *entire* encrypted private key U_K along with a public key V and a proof value proof_{PK_m} are stored on each of the n servers. (Jablon; paragraph 82) Accordingly, Applicants respectfully submit that independent claim 6, as amended distinguishes over the Jablon reference.

Independent claims 17 and 21, both as amended recite similar limitations to independent claim 6, as amended. Accordingly, Applicants respectfully submit that independent claims 17 and 21, both as amended, distinguish over Jablon for reasons similar to those set forth above with respect to independent claim 6, as amended.

Claims 7-9, 18-20, and 22-24 are directly or indirectly dependent from independent

claims 6, 17, and 21, all as amended, respectively. Accordingly, Applicants respectfully submit that dependent claims 7-9, 18-20, and 22-24, distinguish over Jablon for the same reasons discussed above with respect to independent claims 6, 17, and 21, all as amended.

Independent claim 10 recites:

A method of receiving a first password of a user, the method comprising:
entering a second password of the user;
authenticating the user at each of a plurality of servers based on the second password, the plurality of servers being independent from one another;
receiving an encrypted version of a portion of the first password from each of the plurality of servers at which the authentication was successful, each of the portions of the first password containing less than the entire password;
decrypting the received encrypted portions of the first password using encryption keys based on the second password; and
assembling the first password from the decrypted portions.

The Jablon reference does not disclose, teach or suggest the method specified in independent claim 10. First, independent claim 10 recites similar limitation to independent claim 6, as amended. Specifically, Jablon does not teach a method that includes “*receiving an encrypted version of a portion of the first password from each of the plurality of servers at which the authentication was successful, each of the portions of the first password containing less than the entire password.*” Accordingly, Applicants respectfully submit that independent claim 10 distinguishes over Jablon for reasons similar to those set forth above with respect to independent claim 6, as amended.

In addition, independent claim 10 distinguishes over Jablon because unlike the method specified in independent claim 10, Jablon does not teach a method that includes “*decrypting the received encrypted portions of the first password using encryption keys based on the second password.*” Although Jablon teaches that a client 101 chooses a PIN code P which is used to

authenticate the user at the server in the single server system, AM1, PIN code P is not used to decrypt the first password. Rather Jablon teaches that a master encryption key K and a session encryption key K_2 are used to decrypt the private key E_c . (*Jablon; paragraphs 280-283*) Accordingly, Applicants respectfully submit that independent claim 10 distinguishes over the Jablon reference.

Independent claim 25 recites similar limitations to independent claim 10. Accordingly, Applicants respectfully submit that independent claim 25 distinguishes over Jablon for reasons similar to those set forth above with respect to independent claim 10.

Claims 11-13, and 26-28 are directly or indirectly dependent from independent claims 10 and 25, respectively. Accordingly, Applicants respectfully submit that dependent claims 11-13 and 26-28, distinguish over Jablon for the same reasons discussed above with respect to independent claims 10 and 25.

Independent claim 14, as amended, now recites:

A method of authenticating a user at a remote computer system comprising:
dividing a password entered by the user into a plurality of pieces;
transmitting each piece of the plurality of pieces to corresponding ones of a plurality of remote servers, each of the plurality of remote servers being independent from others of the plurality of remote servers, and each of the remote servers having a respective piece of the plurality of pieces of the password pre-registered with the remote server;
comparing the transmitted piece of the plurality of pieces of the password to the pre-registered piece of the password at the plurality of servers;
generating an authentication accept message at each of the plurality of servers at which the pre-registered piece of the password matches the transmitted piece of the plurality of pieces of the password; and
authenticating the user when the authentication accept message is generated for all of the plurality of pieces of the password at the plurality of servers.

The Jablon reference does not disclose, teach or suggest the method specified in independent claim 14, as amended. Unlike the method specified in independent claim 14, as

amended, Jablon does not teach a method that includes ***“dividing a password entered by the user into a plurality of pieces.”***

Instead, Jablon teaches that a master symmetric key K_m is divided into n shares and used to derive a symmetric key which is used to encrypt the users private key U , *in its entirety*, resulting in an encrypted private key U_K . (Jablon; paragraphs 82-85) This is distinct from dividing a password entered by the user into a plurality of parts.

In addition, the Jablon reference fails to teach a method including ***“transmitting each piece of the plurality of pieces to corresponding ones of a plurality of remote servers, each of the plurality of remote servers being independent from others of the plurality of remote servers, and each of the remote servers having a respective piece of the plurality of pieces of the password pre-registered with the remote server.”*** Instead, Jablon teaches that the entire encrypted private key U_k is transmitted to each of the n servers in its entirety. Accordingly, Applicants respectfully submit that independent claim 14, as amended, distinguishes over the Jablon reference.

Claims 15 and 16 are directly or indirectly dependent from independent claim 14, as amended. Accordingly, Applicants respectfully submit that dependent claims 15 and 16 distinguish over Jablon for the same reasons discussed above with respect to independent claim 14, as amended.

///

///


///

///

Applicants respectfully submit that the claims are in condition for allowance. If for any reason the Examiner finds the application other than in condition for allowance, the Examiner is requested to call the undersigned attorney at the Los Angeles, California telephone number (213) 488-7100 to discuss the steps necessary for placing the application in condition for allowance should the Examiner believe that such a telephone conference call would advance prosecution of the application.

Respectfully submitted,
PILLSBURY WINTHROP LLP

Date: June 17, 2004

By: 
Roger R. Wise
Registration No. 31,204
Attorney For Applicants

725 South Figueroa Street, Suite 2800
Los Angeles, CA 90017-5406
Telephone: (213) 488-7100
Facsimile: (213) 629-1033